US005848159A

[11] **Patent Number: 5,848,159**

[45] **Date of Patent: Dec. 8, 1998**

4,405,829	9/1983	Rivest et al. .	
4,424,414	1/1984	Hellman et al. .	
4,514,592	4/1985	Kawamura et al.	380/28 X
4,995,082	2/1991	Schnorr	380/23
5,046,094	9/1991	Kawamujra et al.	380/28 X
5,321,752	6/1994	Iwamura et al.	380/28 X
5,351,298	9/1994	Smith	380/30

OTHER PUBLICATIONS

*RSA Moduli Should Have 3 Prime Factors** by Captain Nemo. No Date or Publication Given.
International Search Report (PCT). ISA/US: Apr. 6. 1998.

Primary Examiner—Bernarr E. Gregory
Attorney, Agent, or Firm—Robert J. Bennett. Esq.; Townsend & Townsend & Crew LLP

[57] **ABSTRACT**

A method and apparatus are disclosed for improving public key encryption and decryption schemes that employ a composite number formed from three or more distinct primes. The encryption or decryption tasks may be broken down into sub-tasks to obtain encrypted or decrypted sub-parts that are then combined using a form of the Chinese Remainder Theorem to obtain the encrypted or decrypted value. A parallel encryption/decryption architecture is disclosed to take advantage of the inventive method.

13 Claims, 2 Drawing Sheets

United States Patent [19]

Collins et al.

[54] **PUBLIC KEY CRYPTOGRAPHIC APPARATUS AND METHOD**

[75] Inventors: **Thomas Collins**, Saratoga; **Dale Hopkins**, Gilroy; **Susan Langford**; **Michael Sabin**, both of Sunnyvale, all of Calif.

[73] Assignee: **Tandem Computers, Incorporated**, Cupertino, Calif.

[21] Appl. No.: **784,453**

[22] Filed: **Jan. 16, 1997**

Related U.S. Application Data

[60] Provisional application No. 60/033,271, Dec. 9, 1996.

[51] **Int. Cl.**[6] **H04L 9/30**; H04L 9/00

[52] **U.S. Cl.** **380/30**; 380/9; 380/29; 380/49

[58] **Field of Search** 380/9, 28, 29, 380/30, 49, 50

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,200,770 4/1980 Hellman et al. .
4,218,582 8/1980 Hellman et al. .